REMARKS

Claims 1-41 are currently pending in the subject application, and are presently under consideration. Favorable reconsideration of the application is requested in view of the comments herein.

REJECTION OF CLAIMS 1-41 UNDER 35 U.S.C. §103(a)

Claims 1-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Kung (U.S. Patent No. 5,241,594) in view of IBM disclosure bulletin (U.S. No. NN880530). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 1, 20 and 31 recite a one-way encrypted password file, installed on each computer in a network, that includes a plurality of user identifications, associated one-way encrypted passwords, and associated privileges for each authorized user. Once the user is logged in, messages (*e.g.*, broadcast messages, multicast messages) that are transmitted across the network are filtered and those messages permitted by the user's associated privileges are displayed or viewed to the user when a match is found on the one-way encrypted password file.

The cited art fails to teach or suggest a one-way encrypted password file that contains privilege information therein, such that the privilege information determines which messages transmitted across a network are viewable by a user based on a user's associated privilege information. Specifically, neither Kung nor the IBM disclosure bulletin teaches or suggests a system where messages are filtered according to user privileges and displayed to an authenticated user. The Office Action suggests that this limitation is met within the Kung reference by the authentication messages provided by

the server to the user's computer. It is respectfully submitted that the authentication messages are neither displayed nor filtered according to user privileges within the meaning of the claims.

Kung discloses a method of authenticating users in a distributed networked computer system. The object of the Kung invention is to allow users to log into multiple remote hosts without the necessity of reentering authenticating information. In one embodiment, a database of user names and passwords are maintained in encrypted form within a database connected to a network server. Once the user has provided authenticating information to the server, the server authorizes a multiple login routine on the user's computer to provide any necessary authentication information to remote hosts.

In an alternate embodiment, user names and passwords are stored in encrypted form on a plurality of computers connected by a secure connection. Each computer contains a secure communication routine by which it communicates with the other computers on the network. When services are desired from a remote host, authentication information is provided to the remote host by this secure communication routine.

The IBM disclosure bulletin discloses a one-way encryption scheme for a system of networked computers. The Office Action cites the bulletin solely for this teaching. The IBM disclosure bulletin does not alone nor in combination with Kung make obvious a one-way encrypted password file provided to each computer in a network that contains privilege information that determines the messages that will be displayable or viewable by the authenticated user.

The authentication message referred to in the Kung merely notifies the user's computer that the user has been authenticated and allows access to software and data within the network. The authentication message is a communication between computers, specifically a message to the multiple logon procedure that it may automatically provide authentication information upon later requests. Such a communication would take the form of a prearranged code within the network that would have no meaning to a human observer. It does not take the form of messages broadcast across the network to all user's in which only those having the associated privileges can view or receive the messages at a respective computer in which they have logged on and have been authenticated.

Similarly, there is no teaching that the messages are filtered according to user privileges. The Kung patent simply does not discuss limiting access to data, software, or messages according to different level of user privileges contained within a one-way encrypted password file. The computer of any user attempting to log in will receive the same authentication message as that of any other user. There is no stored information in Kung as to selective privileges for an authenticated user, making it impossible for Kung to filter messages on this basis. It is respectfully submitted that claims 1, 20 and 31 are nonobvious and patentable over the cited art.

Turning to the dependent claims, Applicant asserts that each dependent claim has its own specific elements and features that define patentable invention over the cited references. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claim 3 recites notification to a systems administrator or security officer of the failure of the user to provide a user identification and a one-way encrypted password that matches a user identification and a one-way encrypted password stored on the one-way encrypted password file. The Kung reference does not discuss transmitting notification of failed log-in attempts to a system operator. The Office Action cites the user log-in rejection function within the Kung system, where a failed log-on attempt causes the server to reject the log-in attempt and wait for another service request. It does not suggest, however, sending notification to a human operator of the failed log-in. Neither reference teaches or suggests a notification to a system operator to report failed log-in attempts. Neither system seeks human intervention.

Claim 5 recites spoofing including the presentation of false messages and information to the user in response to a request by the system administrator or security officer. Neither of the cited references teach providing an unauthenticated user with false data in any form. The Office Action cites the ability of the Kung system to deny access to an unauthenticated user, but this amounts to no more than refusing to accept an incorrect password. The idea of providing false information to mislead an unauthenticated user is not suggested by this rejection.

Claim 6 recites disabling the computer system to prevent access by the user upon a request by the system administrator. Neither cited reference contains a teaching of disabling the system upon one or more rejections of user provided authentication. As discussed above, the Kung system merely loops the user back to an entry screen upon a failed password. The IBM reference merely logs such attempts to aid in identifying the individual responsible.

Claim 7 recites deleting a plurality of files from the computer system upon a request by the systems administrator or security officer. Neither reference discusses remotely deleting system files to prevent an unauthorized user from accessing them. The portion of the reference cited in the Office Action describes communications between the host computer and the server, but does not discuss direct action by a system administrator nor the deletion of system files for security purposes.

Claim 8 recites displaying a request for reauthentication at the direction of a system administrator or security officer. Claim 9 requires that this reauthentication will take the form of a displayed log-in screen having a position for entry of the user identification and password. The Office Action cites a passage describing an initial log-in procedure in rejecting these claims. Claims 8 and 9, however, discuss reauthentication, requiring an already authenticated user to reenter a user identification and password upon the request of a system administrator. Neither of the cited references discusses such a reauthentication process. In fact, the stated purpose of the Kung system was to avoid forcing a user to undergo the authentication process each time the user logged into a new remote host. The reauthenticating user of the present invention is forced to reauthenticate just to maintain the present connection. Forcing the user to log-in multiple times within a single host session would appear repugnant to the basic inventive principle of the Kung system.

Claim 14 recites attaching the master password file to a message, encrypting the message with a private key and passphrase available only to the systems administrator or security officer, and transmitting the message to the plurality of computers. Neither of the cited references contains such a teaching. The Office Action cites the Kung

reference in rejecting this claim. The Kung reference, however, does not teach updating the password files on the individual computers. In fact, this would not be feasible to implement in the Kung device, absent significant changes. The first embodiment of the Kung device has a master password file that each computer uses for authentication. In this embodiment, there is no individual password file on each computer to be updated. In the second embodiment, the master password file is replaced by individual password files on each computer. In this embodiment, there is no master password file from which to update. The master password file of the first embodiment serves the same function as the individual password files of the second embodiment. It would not be obvious to combine the two embodiments to contain both absent the guidance of the present claim. Such a combination would be the product of an improper use of hindsight and/or teach away from the Kung reference.

Claim 14 also requires that the master password file be encrypted using a private key. Neither of the cited references teaches or suggests asymmetric encryption techniques. Nor would the addition of such techniques to the Kung device be obvious. Since Kung relies on a secure connection to pass information between servers, additional encryption of intranetwork communications would be superfluous. No further protection is needed within the network.

Claim 15 further includes decrypting the message using a public key corresponding to the private key, reporting to the system administrator any failure to decrypt the message and replacing the one-way encrypted password file with the decrypted master file. The reasoning advanced under claim 14 applies with equal force

here, as neither reference teaches updating individual password files, nor asymmetric encryption.

Claim 15 further recites that the individual computer notifies the system administrator if it receives a master password file that it cannot encrypt. This is intended to notify the system administrator of any attempts by an intruder to impersonate the system administrator. When the public key for the administrator fails to match the encryption key used for the file, it can be assumed that the file has been tampered with or otherwise falsified. Neither of the cited references teaches or suggests such a verification method. The passage cited in the Office Action discusses the authentication method, but does not address the above.

The dependent claims 21-30 and 32-41 depend directly or indirectly from claim 20 and claim 31, respectively. Many of these claims contain limitations similar to those found in claims 2-19. Accordingly, discussion of these claims will be omitted in the interest of brevity and redundancy. Applicant asserts that claims 21-30 and 32-41 are nonobvious and patentable for the reasons discussed above in the context of claims 2-19.

Additionally, neither reference teaches or suggests a one-way encrypted password file that contains privilege information therein, such that the privilege information determines which messages transmitted across a network are viewable by a user based on a user's associated privilege information as recited in claims 1, 20 and 31. It is thus respectfully submitted that claims 1, 20 and 31 are nonobvious and allowable over the cited art. Claims 2-19, 21-30 and 32-41 depend directly or indirectly

from base claims 1, 20 and 31, respectively. Therefore, claims 2-19, 21-30 and 32-41 are nonobvious and patentable over the cited art.

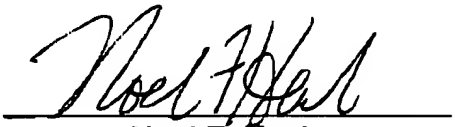
For the reasons described above, claims 1-41 are nonobvious and patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Respectfully submitted,

Date: December 5, 2002



Noel F. Heal
Registration No. 26,074

TRW INC.
Intellectual Asset Management
One Space Park, E2/6051
Redondo Beach, CA 90278
Telephone: (310) 823-4910
FAX: (310) 812-2687